Overview of my|CalPERS
System Access Administration

TABLE OF CONTENTS

1. Introduction to System Access Administration

my|CalPERS provides our business partner community with a powerful tool for conducting business with CalPERS. Each business partner will have the ability to submit, correct and/or view information based on appropriate access privileges. my|CalPERS relies on each business partner to manage the assignment and maintenance of these privileges for their staff, and these activities are collectively referred to as system access administration. System access administrator pages are available within my|CalPERS to allow the set up of users, establishment of initial passwords, and the assignment of user roles.

1.1   System Security

System security features in my|CalPERS have been designed to ensure your data is secure and that you can properly and safely assign access to the system, make updates to your business partner profile, update your business contacts information and capture business partner reporting relationships within my|CalPERS.

CalPERS is committed to protecting your confidential information, and it has taken extra steps to do so. For that reason, each my|CalPERS system user at your agency, as designated by your system access administrator, will be required to review and agree to an online CalPERS Security Agreement when registering for an account.

CalPERS will be introducing enhanced security features that include:

- Data encryption over secured internet connections

- Password authentication to ensure that only your appropriate personnel are accessing sensitive organization and participant data

- System time-outs, set by CalPERS, that automatically log a user off the system after long periods of system inactivity

- The ability to establish business partner relationships. my|CalPERS will allow an authorized third party to submit information on behalf of a CalPERS employer or for a direct authorization agreement.

1.2   Role and Responsibilities of System Access Administrator

The process of using account administrators will be familiar if you are an employer and already use the Automated Communications Exchange System (ACES). With the new system, each business partner will designate one or more my|CalPERS system access administrators. These system access administrators are similar to the ACES user account administrator roles employers use today; however, with my|CalPERS, your

ability to control the roles that you allow for your internal staff will be expanded and improved.

The system access administrator refers to the role of an individual who has responsibility for the management of user access to my|CalPERS. In this context, it is the agency's point-of-contact who will be accountable for granting and maintaining user access for all individuals who will be performing business functions with CalPERS via the new system. They also will have the responsibility to reset a user's password, lock a user's access rights to the system, and change a user's system access role(s).

The system access administrator role will have a high level of access to a number of system pages to perform their role. Since this person will be accountable for providing my|CalPERS access to any additional users, they will be using system access administrator pages on my|CalPERS to associate pre-defined system access roles to each contact, and assign them a username and temporary password.

1.2.1 Pre Launch Activities

Each business partner is expected to identify a person within their organization to assume the system access administrator role. You will need to provide profile information on this person to CalPERS as part of your my|CalPERS readiness activities. For file reporters, the profile information must be provided to CalPERS prior to the file readiness testing activities, since it is expected that they will register and establish a username and password for themselves and any users that will participate in file testing. For online reporters, the profile must be provided to CalPERS during a window of time (to be determined) prior to the my|CalPERS launch.

1.2.2 Post Launch Activities

CalPERS will expect the system access administrator to confirm their agency's business contacts, as well as any third party or service provider relationships. Post launch, we expect them to log on with their username and password and assign their staff access as appropriate. Assigning access will also include distributing usernames and passwords to their staff, based on the process best-suited and acceptable to the agency.

1.3   Terms and Definitions

The following terms are referenced in this document:

- **Business Contacts** - Individuals who provide information to CalPERS on behalf of a business partner. They can be either:
  o An individual identified to answer general questions about a specific area, or

- o An individual identified to perform business activities in my|CalPERS (a system user)

- **Business Partner** - Business partners include CalPERS contracted employers, third party service providers that process employer payroll, retirement or health reporting, direct authorization vendors, medical and dental carriers and associations, and third-party administrators. Business partners are considered external stakeholders who will be impacted by the my|CalPERS implementation.

- **Direct Authorization Vendor (DAV)** - An entity that has a deduction processing agreement with CalPERS. The agreement permits CalPERS benefit recipients to authorize deductions from their retirement allowance associated but not limited to membership fees, organization dues, life or health premiums, and credit union payments.

- **File Readiness** - A state in which external business partners demonstrate that they meet the criteria for successfully submitting, validating, and correcting data files

- **File Readiness Testing** - The set of activities that an employer will complete to verify that their new electronic file for submitting data to CalPERS meets the new format and data requirements for retirement enrollment, health enrollment, payroll contribution, and supplemental income plan data and can be successfully transmitted to the new my|CalPERS system

- **File Transfer Protocol (FTP) –** A method of transferring data files from one computer to another over a network. FTP is used to describe one of the my|CalPERS reporting methods whereby a business partner will create a data file and transfer the file to CalPERS via a scheduled process.

- **Service Provider** – A type of business partner that provides services, such as payroll, billing or enrollment services, to other business partners

- **System Access Administration** - The process for providing access to appropriate business partner personnel for my|CalPERS functions that are needed by individuals filling business partner roles and for file readiness testing activities

- **System Access Administrator** - Individual who has responsibility for the management of user access to my|CalPERS

- **Uniform Resource Locator (URL)** – The global address of a specific website or file on the Internet

2. Considerations for Establishing System Access Administration

The following considerations should be taken into account when establishing system access administration for your organization.

2.1 Preparation for Granting System Access to Business Contacts

Prior to setting up business contacts in my|CalPERS, and allowing them to be users by granting them system access, it is advisable that system access administrators conduct some pre-work for the information that will be required by the system. The suggested preparatory activities are as follows:

- Compile a list of all individuals in your organization that will require access to the my|CalPERS system.

- Establish these individuals in my|CalPERS as business contacts, if they are not set up already.

- Identify the conventions that will be used for creating user names, if desired.

- Create a user name for each individual.

- Determine what type of access each individual will require in order to conduct business with CalPERS, and identify which predefined my|CalPERS system access role(s) must be assigned to each individual.

- Be prepared to explain to each individual being granted system access that they will be given a temporary password, which they must change when they log into the system.

2.2 Additional System Access Administrator

Determine whether one or more additional system access administrators are required for your organization. Depending on the size and/or structure of your organization, you may need additional system access administrators to perform one or more of the following functions:

- Provide back-up for the primary system access administrator in the event that this individual is not available to perform the system access administrator activities

- Manage a group of users at another business location

- Manage a group of users that belong to a specific organizational entity

2.3　Service Provider Relationships with Employers

Organizations or individuals can contract to provide services, such as payroll, billing or enrollment services, to other business partners. These types of business partners are known as service providers. When an employer initiates a new relationship with a service provider, the employer must indicate the programs and services that the service provider will provide for the employer's organization. This will identify the specific pages that the service provider can access and actions that the service provider can perform on behalf of the employer.

For payroll, billing or enrollment, the service provider must ensure that they have contacts set up within their profile, and that they have access to do the work associated to the relationship. For example, if a payroll service provider relationship is established, only the payroll contacts for the service provider should be granted access to manage the employer's payroll. In this case, the payroll security access role is assigned to the payroll contacts.

A third party entity which is designated as a service provider can only perform their service provider functions in the context of a single employer at any one time. Therefore, if a service provider has service relationships with multiple CalPERS employers, the service provider must log into the my|CalPERS system and choose the entity that it needs to conduct business for in the system. They will be able to submit a single file via FTP for multiple employers, but to correct any errors online and view summary information, they will need to log in under the context of a specific employer.

2.4　Sponsors for Direct Authorization Agreements

Sponsors for Direct Authorization Agreements will need to establish system access administrators for their organization. There is a single access role for direct authorization. The functionality available to the user is determined by the relationship defined on the agreement.

2.5　Carrier and Third Party Administrator Relationships with Direct Authorization Agreements

Carriers and/or third party administrators that are associated with direct authorization agreements need to establish system access administrators for their organization. Although there is only one system access role for direct authorization, the relationships specified on the agreement for the sponsor, third party administrator or carrier will identify the specific pages that the parties can access and actions that the parties can perform with respect to the agreement.

3. my|CalPERS System Access Administrator Registration

Registering a system access administrator is a simple online registration process that validates each registrant's profile information, grants access to necessary components of the application, and provides a link to first-time login instructions. As part of the process, each business partner will need to identify a primary point-of-contact to assume the role of my|CalPERS system access administrator. PERT has established a web page on CalPERS On-Line for you to provide this information, called "Identify Your my|CalPERS System Access Administrator." You will receive an email from PERT with instructions on how to access and use this web page.

Each individual identified as a system access administrator will need to register in the my|CalPERS system to establish system access administration for their organization. System access administrators will receive instructions, a registration code, and a URL from CalPERS via email, and must follow the registration process using a series of online pages. The diagram below outlines the registration steps each of these individuals will need to complete prior to assigning access privileges to individuals in their organization.

System Access Administrator Registration Process Steps

Start → Access 'Pre Login'; select 'Business Partner'; and Select 'Continue' → Select 'Register Now' Link on Bottom of Page → Read Registration Instructions and Select 'Continue' → Read Security Agreement and Select 'I Agree' → Enter Registration Code and Select 'Continue' → Review Basic BP Information and Select 'Save & Continue'

Review Address Information and Select 'Confirm' → Review Basic BP Information and Select 'Save & Continue' → Create User Name and Password and Select 'Save' → Registration Confirmation; Click on 'Log In' → Enter Username and Password and Select 'Log In' → Enter Challenge Questions and Answers; Select 'Save and Continue' → Home Page → END

It is important to note that the first time a system access administrator logs into my|CalPERS, after completing the registration process, they will be required to enter five Challenge Questions and Answers. The questions are chosen from drop-down lists and then the answers are entered into the corresponding answer fields. The questions are very simple (for example, "In what city were you born?" or "What is your favorite movie?") and are intended to be easy to answer.

4. Overview of System Access Administration Activities

4.1   Introduction

System Access Administrators have access in my|CalPERS to create and maintain business contacts, grant and maintain system access for business contacts, and establish business partner relationships. Access to perform these functions is contained in the system access administrator role that is assigned to system access administrators.

For CalPERS employers, it should be noted that access to create and maintain business contacts, as well as access to establish business relationships, is also included in the role called employer maintenance. Although it is assumed that a system access administrator would set up a business contact and then grant system access to that contact, it is possible that in some organizations another person, who has been assigned the employer maintenance role, will set up a business contact. Then the system access administrator will grant the system access.

CalPERS employer training on how to perform the functions of a System Access Administrator will be provided via a Computer-Based Training (CBT) module called Profile Maintenance for Employers. The individuals who have been identified as system access administrators will be notified when this CBT becomes available and will be provided with instructions on how and where to register for the CBT.

Training for Direct Authorization Vendors will be provided via Web conference and through a my|CalPERS User Guide specific to the Direct Authorization Vendor processes and roles.

4.2   Creating Business Contacts

Users in the my|CalPERS system are referred to as business contacts. Business contacts provide information to CalPERS on behalf of a business partner. They can be either:

- Someone identified to answer general questions about a specific area, or
- Someone identified to perform business activities in my|CalPERS (a system user)

System access administrators will have to add each contact in my|CalPERS, even if the contacts have previously registered with the existing my|CalPERS or have used ACES.

4.3   Granting System Access and Roles to Business Contacts

To give a business contact access to my|CalPERS, the system access administrator must assign them a user name, system access roles and a temporary password. System access roles indicate which pages a business contact can access and what processes they can do. Refer to the appendices in this document for descriptions of the system access roles:

- Appendix A – System Access Roles for Employers
- Appendix B – System Access Roles for DAVs

4.4   Maintaining System Access for Business Contacts

Miscellaneous maintenance activities are performed as needed by a system access administrator related to a business contact. These activities include the ability to:

- Reset passwords – If a business contact who has been granted system access forgets their password, it can be reset with a new temporary password, which the business contact can then change to a new password.

- Deactivate the business contact – System access for a business contact can be deactivated.

- Reactivate the business contact – System access for a business contact that had been deactivated can be restored by reactivating the business contact.

- Change access privileges for a business contact – System access roles assigned to a business contact can be changed in order to change access privileges.

It is also important that the information stored in the business contact record be kept current as part of ongoing maintenance.

4.5   Establishing Business Partner Relationships - Employers

Business partners that contract with CalPERS can identify another organization to work with CalPERS on their behalf. For example, a CalPERS employer can have another organization report their payroll to CalPERS on their behalf.

In order to have this relationship established in my|CalPERS, both sides must be registered as business partners in my|CalPERS and agree to the CalPERS security agreement. If both sides are already business partners, then the relationship simply needs to be submitted and approved. If only one side is a business partner, the other organization must register as a business partner before the relationship request can be approved. The process for submitting and approving a business partner relationship is still under construction, and the details of the process will be provided as we get closer to my|CalPERS launch.

4.6   Establishing Business Partner Relationships - Direct Authorization Agreements

Business partners that sponsor Direct Authorization agreements with CalPERS can identify another organization to work with CalPERS on their behalf. For example, a sponsor for a direct authorization agreement can have another organization submit deduction requests to CalPERS on their behalf.

In order to have this relationship established in my|CalPERS, all parties to the agreement must be registered as business partners in my|CalPERS and agree to the CalPERS security and hold harmless agreements. If any party related to the agreement has not logged on and accepted the security and hold harmless agreements, the agreement will not be active and deduction requests will not be processed.

5. Adding System Access Administrators

It is recommended that each business partner have a back-up system access administrator. There also may be requirements for additional system access administrators based on a business partner's business model. The designated system access administrator can grant access to the system access administrator role to backup and/or additional system users as needed, in the same way it is currently done in ACES.

6. Available Resources

6.1   PERT Readiness Resources Web Section for Employers

There are many resources available to assist you in preparing for the launch of my|CalPERS. The PERT area of CalPERS On-Line provides valuable information for employers at www.calpers.ca.gov/pert.

In the PERT Readiness Resources Web section, you will find many topics from which to choose. For example, you can view our list of published Frequently Asked Questions (FAQs) to see answers to many of the questions external business partners have already asked relating to the launch of my|CalPERS.

6.2   PERT Readiness Resources Web Section for Direct Authorization

There are many resources available to assist you in preparing for the launch of my|CalPERS. The Business Partner area of CalPERS On-Line provides valuable information for parties associated with Direct Authorization agreements at www.calpers.ca.gov/mycalperspartners.

In the DAV Readiness Resources Web section, you will find many topics from which to choose. For example, you can view our list of published Frequently Asked Questions (FAQs) to see answers to many of the questions external business partners have already asked relating to the launch of my|CalPERS.

6.3   Computer-Based Training (CBT) Module – Profile Maintenance for Employers

Instructions for performing system access administration functions will be contained in the Computer-Based Training (CBT) module – Profile Maintenance for Employers. Information regarding this CBT will be provided on the PERT area of CalPERS On-line when the CBT becomes available. You will find registration instructions to access the CBT to help you learn how to perform the system access administration functions described in this reference guide.

6.4   Contact PERT

If you would like to contact a PERT representative for assistance, please email us at CalPERS_PERT4U@calpers.ca.gov

If you would like to contact a CalPERS Employer Representative for questions or assistance with system access administration, please phone the Employer Contact Center toll-free at **888 CalPERS** (or **888**-225-7377).

Appendix A - System Access Roles for Employers

Access roles define access to my|CalPERS. It is the responsibility of each Business Partner to manage the assignment of these privileges for their staff.

SYSTEM ACCESS ROLES FOR EMPLOYERS (sample list)	
Roles	These Roles allow a user to
System Access Administrator	Assign and maintain access privileges to an employer's staff. Add and maintain contact information and reporting relationships.
Employer Inquiry	View and search employer and employee information related to the employer.
Employer Maintenance	Add and maintain contact information. Maintain employer demographic information as well as set up and maintain reporting relationships.
Retirement Contracts	Initiate, maintain, and terminate new agency retirement agreements and Social Security Medicare-Only agreements. School District reorganizations and mergers, as well as Golden Handshake resolutions, can be submitted by a user with these access privileges.
Health Contracts	Initiate, maintain, or terminate an employer's health contract. The user will be able to submit qualifying information for their organization's eligibility to enter into a health contract.
Supplemental Income Plan	Initiate, maintain and terminate a supplemental income plan agreement. The user will be able to submit qualifying information for their organization's eligibility to enter into a supplemental income plan.
Payroll	Submit their organization's payroll reports to CalPERS. They will also be able to correct and edit any payroll records submitted in error.
Health Enrollment	Process health enrollment transactions for their active employees, including initial health enrollment, enrollment changes or updates due to life events, as well as health enrollment termination.
Retirement Enrollment	Process retirement enrollment and appointment information, including maintaining appointments and enrollment information in relation to the programs for which their organization are contracted.
Service Credit Purchase (SCP) Certification	Submit employee history in support of member SCP request.
Accounts Payable/Billing	Review contribution payment and health premium billing information and make payments.
Direct Authorization	Initiate, maintain, and terminate direct authorization agreements between the employer and their direct deduction processor. If they process the deductions, the user is able to submit, edit, and delete deduction records as well as view and print deduction registers.
Retirement Enrollment Read Only	Read-only access to retirement enrollment and appointment information.
Health Enrollment Read Only	Read-only access to health enrollment transactions.
Accounts Payable/Billing Read Only	Read-only access to contribution payment and health premium billing information.

Appendix B – System Access Roles for DAVs

SYSTEM ACCESS ROLES FOR DAVS (sample list)	
Roles	These Roles allow a user to
System Access Administrator	Assign and maintain access privileges to an employer's staff. Add and maintain contact information and reporting relationships.
Direct Authorization	Initiate, maintain, and terminate Direct Authorization agreements between the employer and their direct deduction processor. If they process the deductions, the user is able to submit, edit and delete deduction records as well as deduction registers.